

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----x

TURRET LABS USA, INC.,

Plaintiff,

MEMORANDUM & ORDER
19-CV-6793 (EK) (RML)

-against-

CARGOSPRINT, LLC and JOSHUA WOLF,
individually,

Defendants.

-----x

ERIC KOMITEE, United States District Judge:

Turret Labs USA, Inc. ("Turret") brings this action against CargoSprint, LLC ("CargoSprint") and its CEO, Joshua Wolf. Turret alleges that the Defendants accessed its proprietary software under false pretenses, then misappropriated its trade secrets.

In its first amended complaint, Plaintiff alleged that Defendants' conduct violated the Racketeer Influenced and Corrupt Organizations Act ("RICO"), the Defend Trade Secrets Act ("DTSA"), and the Computer Fraud and Abuse Act ("CFAA"). That complaint also alleged state-law violations: misappropriation of trade secrets, unfair competition, conversion and defamation.

Defendants moved to dismiss the first amended complaint. Following this, Plaintiff moved to amend; they attached a proposed second amended complaint (the "SAC") to

their motion. The proposed SAC would drop the RICO count; it would also include additional factual allegations as to the remaining claims. Defendants opposed the motion to amend as futile. For the sake of efficiency, Plaintiff's motion to amend is granted and the Court construes Defendants' motion to dismiss as being made against the SAC. For the reasons that follow, the Court grants that motion to dismiss in part and denies it in part.

I. Background

The gravamen of Turret's complaint is that Defendants should never have had access to Turret's proprietary software, because CargoSprint is not the type of business for which the software was intended – namely, a “freight forwarder.” Nevertheless, Defendants allegedly schemed to obtain such access, and ultimately stole Turret's trade secrets to develop a competing product.

The following facts are alleged in the SAC. Turret developed and owns all rights to a logistics-management software program it calls Dock EnRoll. SAC ¶¶ 17-18, 52. The program is designed to facilitate the hand-off of air cargo arriving in the United States to ground transporters, and the payment of associated storage and handling fees. *Id.* ¶¶ 16-17. Dock EnRoll was created for exclusive use by freight forwarders, which are entities that arrange for merchandise to be shipped by

air and stored upon arrival. *Id.* ¶ 16. The program allows freight forwarders to pay “ground handling warehouse operators” and to schedule shipments efficiently “based on synchronized real-time United States Customs release notifications.” *Id.* ¶¶ 16-17. It took two years to create Dock EnRoll, the “first software of its kind,” with twenty-five employees working approximately 132,000 total hours. *Id.* ¶¶ 17-18.

In 2008, Turret entered into an exclusive licensing agreement with Lufthansa Cargo Americas (“Lufthansa”). *Id.* ¶ 19. This agreement allowed Lufthansa, a cargo airline, to provide Lufthansa’s customers with access to Dock EnRoll. *See id.* ¶¶ 19-20. Turret gave Lufthansa complete control over “who could access and use Dock EnRoll.” *Id.* ¶ 20; *see also id.* ¶ 21(f) (“User Access for Dock EnRoll is managed by Lufthansa only, and no other party has access without Lufthansa’s authority.”). However, Turret alleges that pursuant to the licensing agreement, “Lufthansa would only permit registration to freight forwarders” and that Lufthansa would “restrict[] the authorized access of the registered freight forwarders to . . . specified use[s].” *Id.* ¶¶ 17, 20, 21(i), 21(j). Lufthansa was also “required . . . to adopt strict procedures such as user name and password protections” for freight-forwarding customers. *Id.* ¶ 21(j). These obligations allegedly emanated from two documents – the Lufthansa Information Security Policy and

Lufthansa List of Procedures for Dock EnRoll – which Plaintiff calls the “Security Documents.” *Id.* ¶ 21(d), (e).

Turret claims that it took other protective measures to limit access to Dock EnRoll, including by ensuring that:

- Dock EnRoll’s “[d]evelopment, test, and production environments reside in a secure Mindshift Datacenter . . . with constant monitoring”;
- “[a]ll servers are locked in monitored cages” that staff “need to pass biometric scanning” to access;
- “[o]perational control and network governance of the assets residing in the Mindshift Datacenter are protected through” the Security Documents; and
- the “Front-End user interface of Dock EnRoll is accessible only via encrypted HTTP/SSL tunnels.”

Id. ¶ 23(a), (b), (d), (e).

The SAC refers to the licensing agreement and Security Documents only generally, however, pointing to no specific provisions in these documents. While Turret alleges generally that pursuant to the licensing agreement, “Lufthansa would only permit registration to freight forwarders,” see ¶¶ 21(i), 17, it does not specifically allege that any particular provision of

the software licensing agreement, the Security Documents, or any other document required Lufthansa to do so.¹

At oral argument on CargoSprint's motion to dismiss the first amended complaint, the Court pressed Turret's lawyers to clarify the nature of Lufthansa's obligation to "strictly" limit access to Dock EnRoll only to freight forwarders. Specifically, the Court attempted to drill down on whether Turret was alleging a contractual duty. Turret's attorney responded:

[W]e could amend [the first amended complaint] and represent that there was a protocol in place to ensure that the parties using the program were freight forwarders. Whether I could allege that there was a binding contract, I don't think that's required under the law. I think it's more of a representation that would be required.

Transcript of Oral Argument at 26:15-21 (Aug. 14, 2020).

Despite this colloquy, the proposed SAC does not contain any specific allegation about a "protocol" in place. Instead, it avers simply that "based on Lufthansa's protocols, no freight forwarder or other user would have been granted access to . . . the platform." SAC ¶ 31. Nor does the SAC plead any new and specific factual content concerning the nature of Lufthansa's obligation to limit access to Dock EnRoll –

¹ The SAC also mentions a "Dock EnRoll Rule Book," but does not describe what that document contains. See *id.* ¶ 79.

instead, it adds the general statement that "Pursuant to the licensing agreement, Lufthansa would control who could access and use Dock Enroll." *Id.* ¶ 20. And despite the colloquy above, the SAC makes no allegation whatsoever concerning "representations" that Lufthansa solicited or obtained from users.

CargoSprint is not in the freight forwarding business, according to Turret. *Id.* ¶ 26 (describing CargoSprint as a "payment processing company"). Nevertheless, and despite the alleged security precautions discussed above, CargoSprint was able to gain "unfettered" access to Dock EnRoll. *Id.* ¶ 31. Turret alleges that CargoSprint used this unauthorized access to "steal Dock EnRoll's trade secrets involving algorithms, calculations, design patterns, and methods of dock availability schedule optimization." *Id.* ¶ 25.

It is unclear when and how CargoSprint obtained access to Dock EnRoll. Plaintiff alleges that in 2014, Joshua Wolf, CargoSprint's CEO, "contacted" Turret's CEO and falsely "represented that CargoSprint . . . was registered as a freight-forwarder." *Id.* ¶ 23. Turret does not, however, allege that CargoSprint gained access to Dock EnRoll as a result of this misrepresentation. Instead, Turret frames the possible means of CargoSprint's access in the alternative: CargoSprint accessed Dock EnRoll either "through Lufthansa" by "[f]alsely holding

themselves out as a freight forwarder,” or by using the existing log-in credentials of a freight forwarding company called “Damco.” *Id.* ¶ 71; *see also id.* ¶ 24. Plaintiff alleges that CargoSprint went on to gain access “through a Lufthansa employee” to “technical information and [] algorithms[,]” and that no customer should have been given such “expansive” access. *Id.* ¶¶ 30-31, 34.

CargoSprint allegedly “reverse engineer[ed]” this technical information to develop an “identical,” competing software called “SprintPass,” which it unveiled in 2018. *Id.* ¶ 29. Turret claims that CargoSprint misappropriated its trade secrets, including the software’s “methodology for organizing and accumulating data” from “air cargo electronic handling systems”; “computing . . . solutions” that coordinate “dock availability . . . for forwarder’s [sic] truck pickups”; scheduling systems that “optimiz[e] available docks for dangerous cargo and perishables pickup”; programs that facilitate U.S. Customs clearance; and algorithms consisting of “storage charge and fee storage calculations.” *Id.* ¶¶ 30, 54(a)-(f). SprintPass’s features also include “a direct encrypted tunnel to U.S. Customs,” a function no competing program besides Dock EnRoll had previously offered, as well as Dock EnRoll’s “dock schedule optimization” and “terminal fee payment” features. *Id.* ¶ 36.

As a result of competition from SprintPass, Turret's business is suffering. *See, e.g., id.* ¶ 49. SprintPass offers its service free to customers that sign an exclusivity agreement. *Id.* ¶ 38. Turret alleges that CargoSprint is profiting further by disparaging Turret's offering. Plaintiff claims that in 2018, defendant Wolf approached certain companies "involved in business dealings" with Plaintiff and "told them that the SprintPass system did everything Dock EnRoll did and was superior to Dock EnRoll and that Lufthansa would soon be terminating its agreement with Plaintiff." *Id.* ¶ 39. As a result, one of those companies – Mercury Air Cargo – stopped using Dock EnRoll and began using SprintPass. *Id.* ¶¶ 40-41. Lufthansa did not, however, actually terminate its contract with Turret. *Id.* ¶ 42.

II. Legal Standards

A. Motion to Amend

It is well-settled that when a plaintiff seeks to amend the complaint while a motion to dismiss is pending, the Court has a variety of options. *E.g., Kilpakis v. JPMorgan Chase Fin. Co., LLC*, 229 F. Supp. 3d 133, 139 (E.D.N.Y. 2017). If the proposed amendments "d[o] not seek to add new claims or parties, and the Defendants have had a sufficient opportunity to respond . . . then, for the purposes of procedural efficiency, the merits of the pending motion to dismiss ought to be

considered in light of the proposed amended complaint.” *Id.* (collecting cases); *see also, e.g., S.F. v. Archer-Daniels-Midland Co.*, No. 13-CV-634S, 2014 WL 1600414, at *1 (W.D.N.Y. Apr. 21, 2014) (granting the motion to amend and construing the motion to dismiss against the amended complaint), *aff'd*, 594 F. App'x 11 (2d Cir. 2014).

Turret's proposed SAC does not bring new causes of action (instead, it removes one) or add new parties. Defendants filed a letter opposing the motion to amend, reiterating many of the arguments from their motion to dismiss the first amended complaint. Further, Defendants responded to the SAC itself, arguing that the amendment would be futile in light of the insufficiency of the allegations as supplemented. *See, e.g., Dougherty v. Town of N. Hempstead Bd. of Zoning Appeals*, 282 F.3d 83, 87 (2d Cir. 2002) (standard for assessing futility is whether the proposed amendments could withstand a motion to dismiss under Rule 12(b)(6)). Therefore, for the sake of efficiency, the Court grants the motion to amend and construes Defendants' motion to dismiss as against the SAC.

B. Motion to Dismiss

In reviewing a Rule 12(b)(6) motion, the Court must accept all factual allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor. *See Lundy v. Catholic Health Sys. of Long Island Inc.*, 711 F.3d 106, 113

(2d Cir. 2013). However, only “a plausible claim for relief survives a motion to dismiss.” *LaFaro v. N.Y. Cardiothoracic Grp., PLLC*, 570 F.3d 471, 476 (2d Cir. 2009). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). However, conclusory allegations are “not entitled to be assumed true.” *Id.* “A pleading that offers labels and conclusions or a formulaic recitation of the elements of a cause of action will not do.” *Id.* (internal quotations omitted).

III. Discussion

A. Defend Trade Secrets Act

The Defend Trade Secrets Act provides a federal cause of action for trade-secret misappropriation involving a nexus to interstate commerce. 18 U.S.C. § 1836(b). To establish the existence of a trade secret, a plaintiff must demonstrate, as a threshold matter, that the property in question is comprised of “financial, business, scientific, technical, economic, or engineering information” including “formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes.” 18 U.S.C. § 1839(3). The plaintiff must then satisfy two additional statutory requirements: First, the owner of the purported trade secret must have “taken reasonable

measures to keep such information secret,” and second, the information must “derive[] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.” *Id.* § 1839(3)(b). Here, Turret’s SAC fails as a matter of law because it has not adequately alleged that it took reasonable measures to keep its information secret from third parties.

In evaluating reasonable secrecy measures, courts in this Circuit generally look to whether confidentiality or nondisclosure agreements are in place and whether the information is guarded by physical- or cyber-security protections. *See, e.g., Charles Ramsey Co., Inc. v. Fabtech-NY LLC*, No. 118-CV-0546, 2020 WL 352614, at *16 (N.D.N.Y. Jan. 21, 2020) (citing cases). The DTSA “does not provide further guidance on what constitutes ‘reasonable measures’ to keep the information secret, and the Second Circuit has not yet construed this statutory term.” *Xavian Ins. Co. v. Marsh & McLennan Companies, Inc.*, No. 18-CV-8273, 2019 WL 1620754, at *4 (S.D.N.Y. Apr. 16, 2019). What measures are “reasonable” must depend in significant part on the nature of the trade secret at issue. *E.g., ClearOne Comm'ns, Inc. v. Bowers*, 643 F.3d 735, 768 (10th Cir. 2011) (“There is no precise definition of what

'reasonable measures' are; what is reasonable depends on the situation."); *Adler v. Loyd*, No. 20-CV-00048, 2020 WL 6060302, at *8 (D.D.C. Oct. 14, 2020) ("A reasonable measure depends on the circumstances, not any bright-line rule.").

Here, the alleged trade secret consisted primarily, if not entirely, of the product's functionality – functionality that is made apparent to all users of the program. In such a circumstance, the physical security of the plaintiff's own servers are mostly beside the point, and the "reasonable measures" analysis must focus heavily on who is given access, under what contractual arrangements, and with what attendant disclosures and representations. This was the case, for example, in *Broker Genius, Inc. v. Zalta*, 280 F. Supp. 3d 495 (S.D.N.Y. 2017), where the plaintiff alleged that the functionality of its "AutoPricer v.3" software constituted a trade secret. The *Broker Genius* court began by recognizing that "the UX/UI [user experience / user interface] of AutoPricer v.3 is made readily apparent to every single user of the software." *Id.* at 517. The court went on to deny Broker Genius's motion for a preliminary injunction, holding that it was unlikely to succeed on the merits without establishing that a contractual duty of confidentiality ran to the software's users. *Id.* at 498 (noting that "Broker Genius discloses the information that it alleges to be its trade secrets to each of its licensees as a

matter of course,” and yet “it has not shown that it required those licensees to maintain the confidentiality of user-facing elements of [its] software”); *Art & Cook, Inc. v. Haber*, 416 F. Supp. 3d 191, 197 (E.D.N.Y. 2017) (reasonable measures not established by trade secret’s owner speaking “to [d]efendant many times about confidentiality” and asking defendant “to sign an employee handbook and non-disclosure agreement . . . though [d]efendant refused to sign”).

The SAC effectively concedes that Turret delegated total control over the sharing of Dock EnRoll to Lufthansa. See SAC ¶ 20 (“Pursuant to the licensing agreement, Lufthansa would control who could access and use Dock EnRoll.”); *id.* ¶ 21(f) (“User Access for Dock EnRoll is managed by Lufthansa only.”). As in *Broker Genius*, every customer that Lufthansa gave access to Dock EnRoll would, by definition, be privy to the functions that Turret calls a trade secret – for example, the functions facilitating scheduling and payment. And absent from the instant complaint is any *specific* allegation that Dock EnRoll’s customers, or Lufthansa, were contractually required to keep Turret’s proprietary information confidential. Turret does allege generally that “Lufthansa would only permit registration to freight forwarders,” SAC ¶ 21(i), and that Plaintiff and Lufthansa were somehow “restricting the authorized access of the registered freight forwarders to . . . specified use[s].” *Id.*

¶ 21(j). However, Turret provides no factual content whatsoever in support of these bald assertions, and invokes no specific provisions of the licensing agreement to support them.

Where a contract's terms are central to a plaintiff's cause of action, the plaintiff has an obligation to plead the contract's terms in sufficient detail to establish a plausible basis for liability. For instance, a breach of contract claim will be dismissed as "too vague and indefinite[]" where the plaintiff fails to allege, in nonconclusory fashion, the essential terms of the parties' purported contract, including the specific provisions of the contract upon which liability is predicated." *Highlands Ins. Co. v. PRG Brokerage, Inc.*, 01-CV-2272, 2004 WL 35439 at *8 (S.D.N.Y. Jan. 6, 2004); *see also*, e.g., *Window Headquarters, Inc. v. MAI Basic Four, Inc.*, No. 91-CV-1816, 1993 WL 312899 at *3 (S.D.N.Y. 1993) (in a breach of contract action, "[a] plaintiff is not required to attach a copy of the contract or plead its terms verbatim," but "must set forth the terms of the agreement upon which liability is predicated") (internal citations omitted)). This principle holds true for trade secret claims as well. *See*, e.g., *Principia Partners LLC v. Swap Fin. Grp., LLC*, No. 18-CV-7998, 2019 WL 4688711, at *3 (S.D.N.Y. Sept. 26, 2019) ("Plaintiff alleges unspecified 'confidentiality obligations,' but fails to describe what those obligations were, how they restrained use of

the software, or how they were violated by Defendant.") internal citation omitted)); *Lawrence v. NYC Med. Practice, P.C.*, No. 18-CV-8649, 2019 WL 4194576, at *5 (S.D.N.Y. Sept. 3, 2019) (allegations that employee agreements contained "trade secret protections" were insufficient where plaintiff pleaded "no further facts regarding these 'trade secret protections'").

Here, as noted, Turret cites to no specific terms of the licensing agreement, despite being a party to that agreement and invoking it in the SAC. See, e.g., SAC ¶ 21(j) (alleging that Turret required Lufthansa to "adopt strict procedures such as username and password protections," but providing no indication where this requirement comes from). And as set out in the Background section, above, Turret's attorney effectively conceded at oral argument that no such contractual arrangement exists, despite Turret's vague reliance on the "licensing agreement" with Lufthansa in the SAC. Nor does Turret point to any specific practices intended to limit access to freight forwarders, whether or not contractually required.

These shortcomings are fatal to Plaintiff's claims. See, e.g., *Mintz v. Mktg. Cohorts, LLC*, No. 18-CV-4159, 2019 WL 3337896, at *6 (E.D.N.Y. July 25, 2019) (DTSA claim failed because plaintiff "did not require defendants to sign a non-disclosure agreement [or] any sort of covenant to protect" the alleged secrets); *Mason v. AmTrust Fin. Servs., Inc.*, No. 19-CV-

8364, 2020 WL 1330688, at *3 (S.D.N.Y. Mar. 23, 2020) (granting 12(b)(6) motion on trade secrets claims where plaintiff did not require any written contract before handing the product in question over to the defendant for its use); *Charles Ramsey*, 2020 WL 352614, at *16 (same, where complaint contained no allegations of contractual confidentiality agreements).

Turret claims that it protected its purported trade secrets through other means, but these protections do not reach the ultimate users of the software or limit their use or sharing of the program. For example, Turret pleads that it locked its servers in monitored cages, and that the data flowing to and from the American, Canadian and Mexican customs services was encrypted on route. SAC ¶ 21(b), (c). The SAC also alleges, nebulously, that certain "Security Documents" contain "[p]rocedures for security and access to users." *Id.* ¶ 21(e); see also *id.* ¶ 21(d) (offering that the Security Documents are confidential and would be produced in discovery). These measures cannot overcome the fact that Turret pleads nothing in respect of Lufthansa's purported obligation to limit access to the program to freight forwarders (or even a de facto practice of limiting access accordingly). Given the nature of the trade secrets at issue, these allegations are akin to a Plaintiff having pleaded that he locked all the upstairs windows of his

house, while remaining silent on whether the front and back doors were left wide open.

Therefore, the SAC does not plausibly plead the existence of a trade secret in the Dock EnRoll software. The DTSA claim is dismissed as a matter of law.

B. Common-Law Misappropriation of Trade Secrets

The elements of a misappropriation of trade secrets claim under New York common law "are fundamentally the same as those sustaining a claim under the DTSA." *See Kraus USA, Inc. v. Magarik*, No. 17-CV-6541, 2020 WL 2415670, at *5 (S.D.N.Y. May 12, 2020) (internal quotations omitted). They require a plaintiff to show "(1) that it possessed a trade secret, and (2) that the defendants used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means." *N. Atl. Instruments, Inc. v. Haber*, 188 F.3d 38, 43-44 (2d Cir. 1999). Therefore, for substantially the same reasons that the SAC fails to plead a DTSA claim, Turret fails to state a claim for misappropriation of trade secrets under New York law.

C. Unfair Competition

Turret fails to state a claim for unfair competition. "A claim for unfair competition based on the same allegations as a claim for misappropriation of trade secrets is treated as a single cause of action." *Uni-Sys., LLC v. United States Tennis*

Ass'n, Inc., 350 F. Supp. 3d 143, 179 (E.D.N.Y. 2018)

(collecting cases). Where, as here, a plaintiff's unfair competition claim is premised on the same allegations as the misappropriation claim, see SAC ¶¶ 77-88, it must be dismissed as duplicative. *Id.*

D. Conversion

Turret also brings a state-law conversion claim. "A conversion takes place when someone, intentionally and without authority, assumes or exercises control over personal property belonging to someone else, interfering with that person's right of possession." *Colavito v. N.Y. Organ Donor Network, Inc.*, 8 N.Y.3d 43, 49-50 (2006). "An essential element of conversion is 'unauthorized dominion' to the exclusion of the rights of the plaintiff." *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 813 F. Supp. 2d 489, 535 (S.D.N.Y. 2011). Cases of "pure copying" do not satisfy the required elements of conversion. *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 415 (S.D.N.Y. 2018). Turret alleges only that Defendants accessed and copied its trade secrets; there is no allegation in the SAC that Plaintiff was deprived of (or excluded from) the use of any component of its software. The conversion claim is therefore dismissed.

E. Computer Fraud and Abuse Act

Under the CFAA, a plaintiff must allege that the defendant "intentionally accesse[d] a protected computer without authorization," and as a result, caused "damage" or "loss" in excess of \$5,000. 18 U.S.C. § 1030(a)(5), (c)(4)(a)(i)(I). Here, Defendants argue that this claim fails because Turret has not plausibly alleged the kind of damage or loss that is cognizable under the CFAA.

The value of stolen intellectual property is not counted towards the CFAA's damage and loss calculation. The statute defines "loss" to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). "Damage" means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Thus, the statute reaches only those losses emanating more directly from the computer intrusion itself: the cost of investigating the intrusion and patching and repairing the system. Moreover, the only lost revenue recoverable under the CFAA is that which is lost because the intrusion has brought down the operations of the victim's

system. "[T]he plain language of the statute treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an 'interruption in service.'" *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 562 (2d Cir. 2006).

Turret's loss allegations in the SAC are conclusory – they say only that "losses are well in excess of \$5,000," and recite the statutory definition for loss. SAC ¶¶ 111, 114. This is insufficient as a matter of law. *See, e.g., Fink v. Time Warner Cable*, No. 08-CV-9628, 2009 WL 2207920, *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because the "allegation merely parrot[ed] the statutory language and [was] thus insufficiently factual to frame plausibly the damages element of Plaintiff's CFAA claim"); *see also Reis, Inc. v. Lennar Corp.*, No. 15-CV-7905, 2016 WL 3702736, at *6 (S.D.N.Y. July 5, 2016) ("Plaintiffs make no allegations that the investigation was for the purpose of looking into any damage to data, programs, or server system, other than the conclusory statement that they 'expend[ed] time, money, and resources (aggregating at least \$5,000 in value) to conduct an investigation into the intrusion and a damages assessment.'"). Plaintiff makes no plausible allegation that it incurred costs in assessing any security breach, *see Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010), or that it lost "good will

or business" from the "impairment or unavailability of data or systems." *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 252 n.12 (S.D.N.Y. 2000). Accordingly, the CFAA claim is dismissed.

F. Defamation

Turret brings a defamation claim with regard to CEO Joshua Wolf's alleged statements to Dock EnRoll customers that SprintPass is "superior" to Dock EnRoll and that "Lufthansa would soon be terminating its agreement with Turret." Under New York law, the elements of oral defamation (i.e. slander) are: "(i) a defamatory statement of fact, (ii) that is false, (iii) published to a third party, (iv) of and concerning the plaintiff, (v) made with the applicable level of fault on the part of the speaker, (vi) either causing special harm or constituting slander per se, and (vii) not protected by privilege." *Sleepy's LLC v. Select Comfort Wholesale Corp.*, 909 F.3d 519, 528 (2d Cir. 2018) (internal quotations omitted).

Statements of opinion cannot be the subject of a defamation claim. *E.g.*, *Gross v. New York Times Co.*, 82 N.Y.2d 146, 152-53 (1993). And defendant Wolf's comment that SprintPass is "superior" to Dock EnRoll is a statement of opinion. *See, e.g.*, *Goldman v. Barrett*, No. 15-CV-9223, 2016 WL 5942529, at *4 n.6 (S.D.N.Y. Aug. 24, 2016) ("[A]ny implication that Plaintiffs are inferior . . . is a non-actionable statement

of opinion; it is merely an expression of one's view of another." (internal quotations omitted)). Accordingly, the claim that that statement was defamatory cannot proceed.

Wolf's statement that "Lufthansa would soon be terminating its agreement with Plaintiff," however, is actionable because it comprises (at least) a mix of opinion and fact. "[A]n opinion that implies that it is based upon facts which justify the opinion but are unknown to those reading or hearing it, is a mixed opinion and is actionable." *Davis v. Boenheim*, 24 N.Y.3d 262, 269 (2014) (cleaned up). Here, a reasonable listener might have inferred that Wolf "had knowledge of facts, unknown to the audience, which support[ed] the assertions [] made." *Kasavana v. Vela*, 172 A.D.3d 1042, 1046 (1st Dep't 2019). The listener might base that inference on Wolf's position in the industry, in part: Wolf and his company had a business relationship with Lufthansa and CargoSprint competed directly with Turret. The listener might also base that inference on the nature of the statement itself. Wolf's alleged choice of words conveys a sense of definiteness – he says that Lufthansa "would" (not might) terminate its relationship with Turret. It also conveys a sense of imminence – that termination would occur "soon." In the circumstances, these aspects of the alleged statement could plausibly suggest to a reasonable listener that Wolf was in possession of facts

unknown to his audience that would support his assertion. See, e.g., *Slue v. New York Univ. Med. Ctr.*, 409 F. Supp. 2d 349, 370 (S.D.N.Y. 2006) (“definite and unambiguous” statements concerning facts known to the speaker were ones of “mixed opinion”).

As to falsity, the SAC pleads that Lufthansa did not, in fact, cease using Dock EnRoll; thus, the statement proved false. Defendants argue, however, that the statement is not actionable because it was a prediction of future events not “capable of being proven true or false” at the time it was uttered. They cite *Finkelstein v. Wachtel*, No. 00-CV-2672, 2003 WL 1918309, at *7 (S.D.N.Y. Apr. 21, 2003), where the court dismissed a slander claim predicated on a lawyer’s statement that the Massachusetts Attorney General “was going to be” involved in a forthcoming investigation and that the investigation would be a “very dirty business.” It is true that “[s]peculations as to the motivations and potential future consequences of proposed conduct generally are not readily verifiable” and cannot be the basis for defamation. *Gross v. New York Times Co.*, 180 A.D.2d 308, 312 (1st Dep’t 1992), *rev’d in part on other grounds*, 82 N.Y.2d 146 (1993). But as alleged, defendant Wolf’s statement goes beyond a mere “prediction” of what might occur in the future for the reasons set out above — namely, the definiteness and imminence in which the statement

was couched. Moreover, whether or not Lufthansa had decided, at that point, to stop using Dock EnRoll was capable of being proven at the time of Wolf's utterance, and may be ascertained in discovery. Accordingly, the defamation claim may proceed over an objection that this statement constitutes mere prediction.

Defendants also argue that the defamation claim fails because Turret has not pleaded special damages, i.e. "the loss of something having economic or pecuniary value." *Rufeh v. Schwartz*, 50 A.D.3d 1002, 1004 (2d Dep't 2008). A complaint that "sets forth damages in round numbers which amount to mere general allegations of lost sales from unidentified lost customers" is insufficient. *Vigoda v. DCA Prods. Plus Inc.*, 293 A.D.2d 265, 266 (1st Dep't 2002). Here, however, the SAC alleges that after Wolf's statement, Mercury Air Cargo stopped using Dock EnRoll and switched to SprintPass. This loss of a named customer is sufficient to plead special damages. *Squire Records, Inc. v. Vanguard Recording Soc. Inc.*, 19 N.Y.2d 797, 798-99 (1967) ("In this action for slander of title or injurious falsehood, special damages are sufficiently alleged because of the specific naming of the customers lost. If further itemization or allocation of damages is required it may be obtained by a bill of particulars or pretrial deposition."); see also *De Marco-Stone Funeral Home Inc. v. WRGB Broad. Inc.*, 203

A.D.2d 780, 781 (3d Dep't 1994) ("When, as here, the special damage claimed is a loss of customers, there must be evidence of particular persons who ceased to be or refused to become customers." (citing *Drug Research Corp. v. Curtis Pub. Co.*, 7 N.Y.2d 435, 440-41 (1960))). Therefore, Turret's defamation claim survives the motion to dismiss.²

IV. Conclusion

For the reasons set forth above, Plaintiff's motion to amend is granted and Defendants' motion to dismiss is construed as against the second amended complaint. Defendants' motion is granted as to Plaintiff's Defend Trade Secrets Act, common-law misappropriation of trade secrets, conversion, unfair competition, and Computer Fraud and Abuse Act claims, and granted in part and denied in part as to Plaintiff's defamation claims.

SO ORDERED.

/s Eric Komitee
ERIC KOMITEE
United States District Judge

Dated: February 12, 2021
Brooklyn, New York

² The defamation claim may proceed in this Court even absent a surviving federal claim because Plaintiff invokes this Court's diversity jurisdiction under 28 U.S.C. § 1332.